
일반 직원들을 위한

보안 패치 업데이트 가이드

안랩 내PC지키미 활용 및 PMS 연동 방안

AhnLab

목차

| | |
|---|----|
| 랜섬웨어 피해 예방을 위한 첫 걸음, 패치 관리 | 3 |
| 1. 백신에 “최신 버전의 엔진” 적용하기 | 4 |
| 2. 윈도우 OS 및 MS 오피스에 최신 보안 업데이트 적용하기 | 4 |
| 3. 한글(한컴 오피스)에 최신 보안 업데이트 적용하기 | 7 |
| 4. 어도비(Adobe) 제품에 보안 업데이트 적용하기 | 8 |
| 직원들이 패치를 적용했는지 확인하려면? | 9 |
| 1. 안랩 내PC지키미로 패치 적용 여부 확인하기 | 10 |
| 2. ‘원클릭’으로 즉각 보안 패치 적용하기: PMS 연동 | 11 |
| 3. 랜섬웨어 피해 예방을 위한 추가 기능: 문서 보호 | 12 |
| 패치 관리부터 임직원 보안 인식 개선까지 | 13 |

랜섬웨어 피해 예방을 위한 첫 걸음, 패치 관리

2017년 5월 13일, 워너크립터(일명 워너크라이) 랜섬웨어가 윈도우 OS의 SMB 취약점을 통해 빠르게 확산되며 전세계 150여 개국의 병원, 일반 기업 및 공공 기관 시스템 30만대를 감염시켰다. 그 보다 앞선 2017년 3월에 마이크로소프트가 해당 취약점에 대한 보안 패치를 배포했음에도 불구하고 기록적인 피해가 발생했다. 지난 10월 25일에는 배드래빗(일명 디스크코더) 랜섬웨어가 유럽 15개국을 중심으로 빠르게 번지면서 국내 보안 관리자들을 긴장시켰다. 배드래빗 랜섬웨어는 주로 드라이브-바이-다운로드(Drive By Download) 방식을 통해 취약한 웹브라우저와 애플리케이션을 사용하는 시스템에 피해를 입혔다.

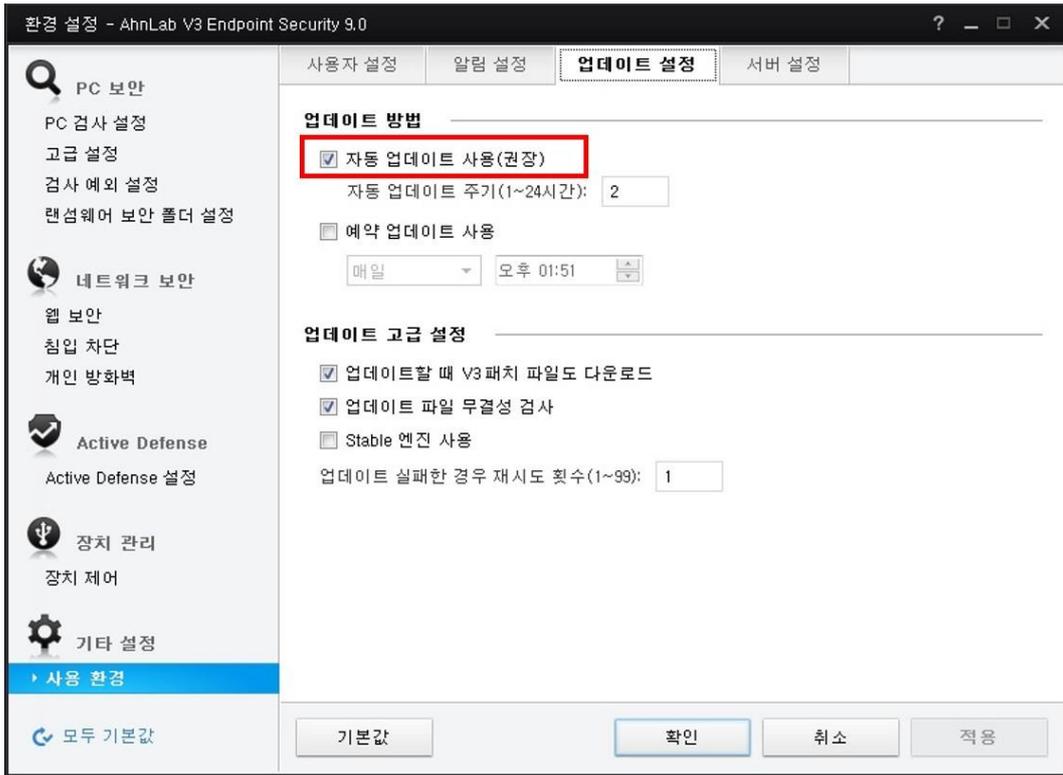
이들 외에도 최근의 굵직한 랜섬웨어 피해 사례를 보면 OS 및 주요 애플리케이션의 취약점을 이용한 공격이 다수를 차지하고 있다. 이에 그 어느 때 보다 패치 업데이트의 중요성이 강조되고 있다. 문제는 임직원들의 실천으로 이어지지 않는 경우가 많다는 것. 특히 컴퓨터 조작성이 익숙지 않은 임직원들이라면 “백신의 엔진을 최신 버전으로 유지하고 사용 중인 애플리케이션의 최신 보안 패치를 업데이트 하시기 바랍니다”라는 공지가 효과를 발휘하기는 어렵다.

그렇다고 보안 관리자가 사내에서 사용되는 OS 및 모든 애플리케이션의 보안 패치를 다운로드하여 자료실을 통해 공유하는 것도 쉽지 않아 결국 직원들이 직접 보안 패치를 설치하도록 유도하는 것이 현실적이다. 그러려면 보안 패치를 다운로드 하는 방법을 가이드해야 하는데, 주요 애플리케이션의 업데이트 방법을 일일이 설명하거나 문서로 만드는 것은 또 다른 번거로움이다. 이런 고민을 덜기 위해 백신 및 주요 업무용 애플리케이션의 패치 적용 방법을 누구나 따라 할 수 있도록 쉽게, 특히 사내 게시판에 그대로 '복사하여 붙여 넣을 수 있도록' 상세하게 정리했다. 또 임직원들이 실제로 보안 패치를 적용했는지 간편하게 확인할 수 있는 방법도 소개한다.

1. 백신에 “최신 버전의 엔진” 적용하기

랜섬웨어를 비롯한 각종 신·변종 악성코드의 감염을 방지하기 위해서는 PC 에 백신을 설치하고 엔진 버전을 항상 최신 상태로 유지하는 것이 필수다. V3 의 엔진 버전을 최신 상태로 유지하려면 '자동 업데이트 사용'만 클릭해두면 된다.

▶ [환경설정(톱니바퀴아이콘)] > [기타설정]-[사용환경]-[업데이트 설정] > [자동업데이트 사용] 체크



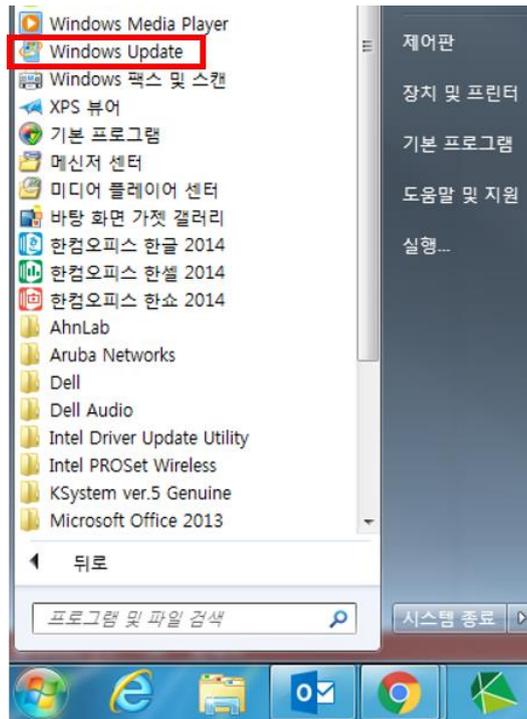
[그림 1] V3 의 '자동 업데이트' 설정

2. 윈도우 OS 및 MS 오피스에 최신 보안 업데이트 적용하기

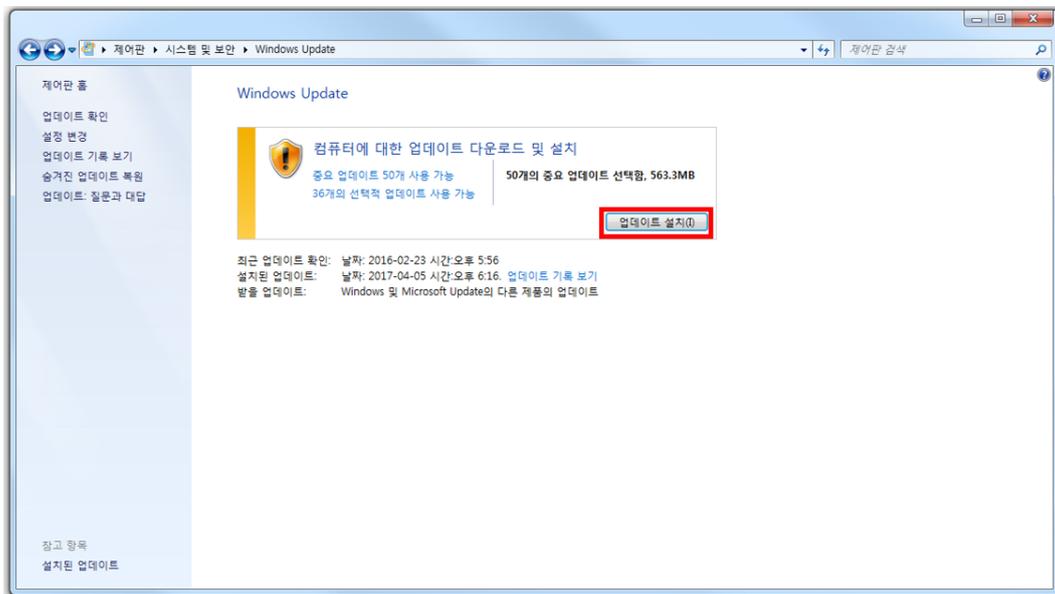
현재 국내 기업 환경에서 가장 많이 사용되고 있는 운영체제인 윈도우(Windows) 7 과 MS 오피스(Office)에 최신 보안 업데이트를 적용하는 방법은 다음과 같다. 매번 업데이트하기 번거롭다면 '자동 업데이트'를 설정하는 것도 방법이다. 단, 기업의 환경에 따라 자동 업데이트가 적절하지 않은 경우도 있어 사전 검토가 필요하다.

■ 윈도우 및 MS 오피스의 최신 보안 업데이트 적용하기 (수동 업데이트, Windows7 기준)

▶ [시작] > [모든 프로그램] > [Windows Update] > [설정 변경] > [업데이트 자동 설치]



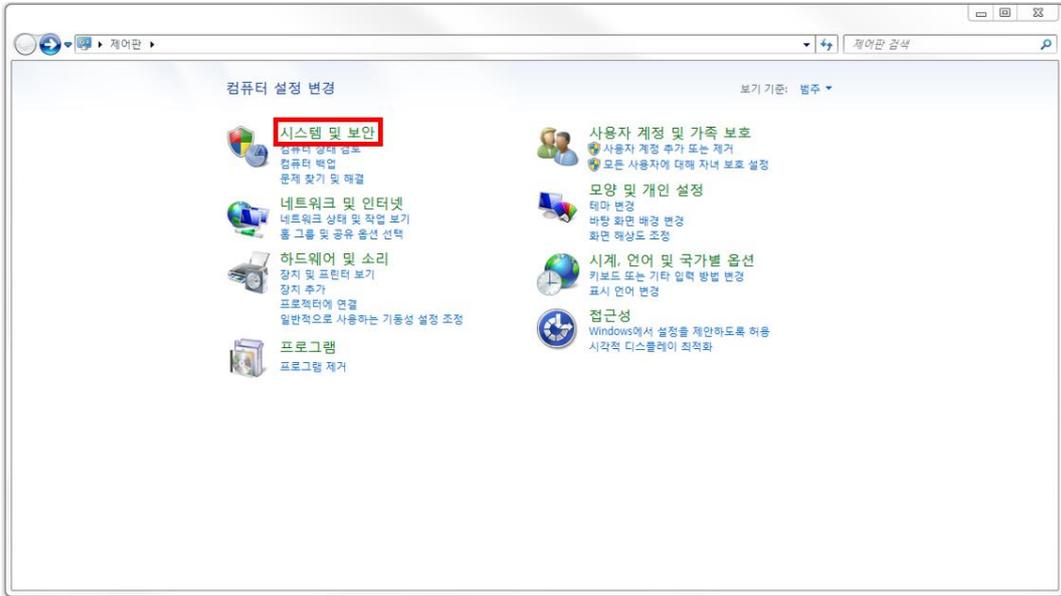
[그림 2] 윈도우 OS [시작] 버튼 > [모든 프로그램] > [Windows Update] 클릭



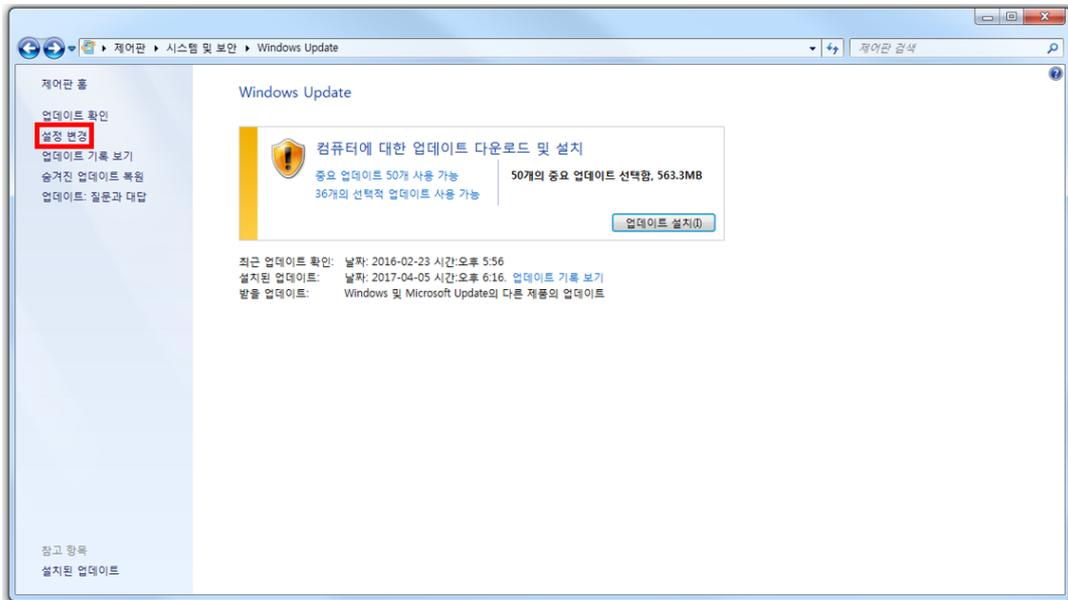
[그림 3] Windows Update 설정창

■ 윈도우 및 MS 오피스의 '자동 업데이트' 설정하기 (Windows7 기준)

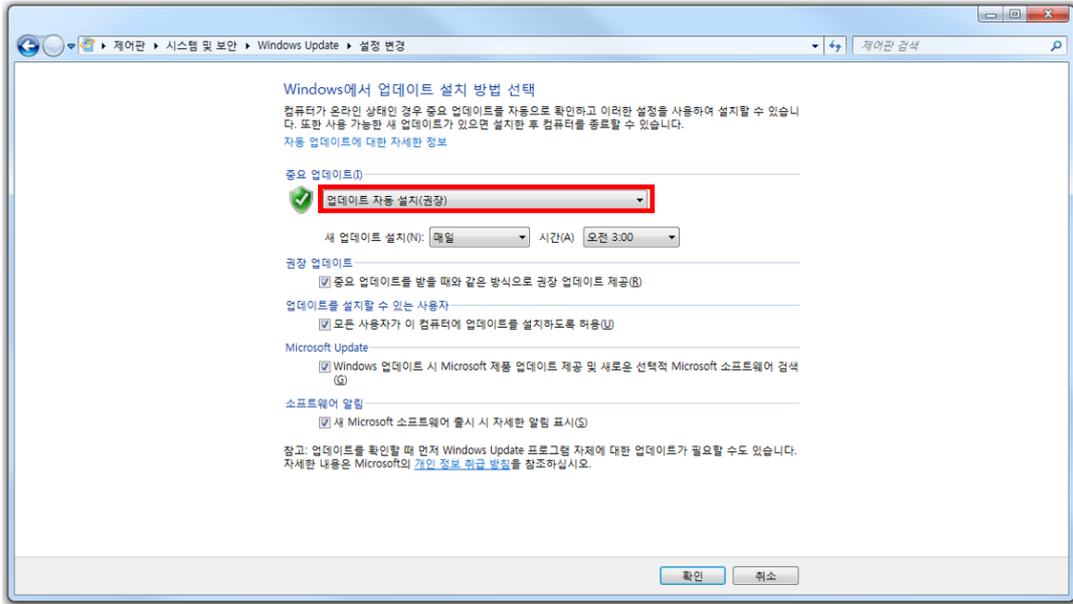
▶ [시작] > [제어판] > [시스템 및 보안] > [Windows Update] > [설정 변경] > [업데이트 자동 설치]



[그림 4] 윈도우 OS 의 [시작] 버튼 > [제어판] > [시스템 및 보안] 클릭



[그림 5] [Windows Update] 창에서 왼쪽 메뉴 중 [설정 변경] 클릭



[그림 6] [Windows Update] > [설정 변경] > [업데이트 자동 설치] 클릭

3. 한글(한컴 오피스)에 최신 보안 업데이트 적용하기

한글(한컴 오피스) 취약점을 이용한 악성코드 유포도 지속적으로 나타나고 있다. 대학 및 주요 공공기관, 병·의원, 금융 기관이라면 한컴 오피스의 최신 보안 업데이트 적용도 반드시 챙겨야 한다. 한컴 오피스의 최신 보안 업데이트 파일은 '한글과컴퓨터(www.hancom.com)' 홈페이지에서 이용할 수 있으며, 번거로울 경우 자동 업데이트를 설정하는 것도 방법이다. 단, 기업의 환경에 따라 자동 업데이트가 적절하지 않은 경우도 있어 사전 검토가 필요하다.

■ 한컴 오피스에 최신 보안 업데이트 적용하기 (수동 업데이트)

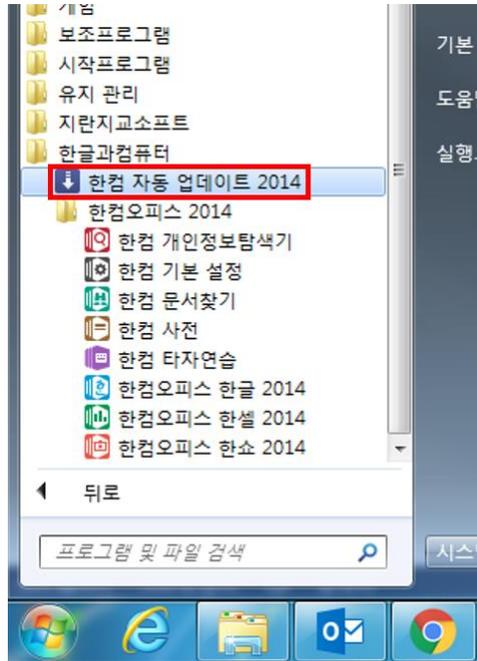
- ▶ 한컴 홈페이지 > [고객지원] > [다운로드] > 해당 제품 패치파일 다운로드 및 실행



[그림 7] 한글과컴퓨터 홈페이지의 '다운로드' 메뉴

■ 한컴 오피스의 '자동 업데이트' 설정하기

▶ [시작] > [모든 프로그램] > [한컴 자동 업데이트] > 자동 업데이트 설정



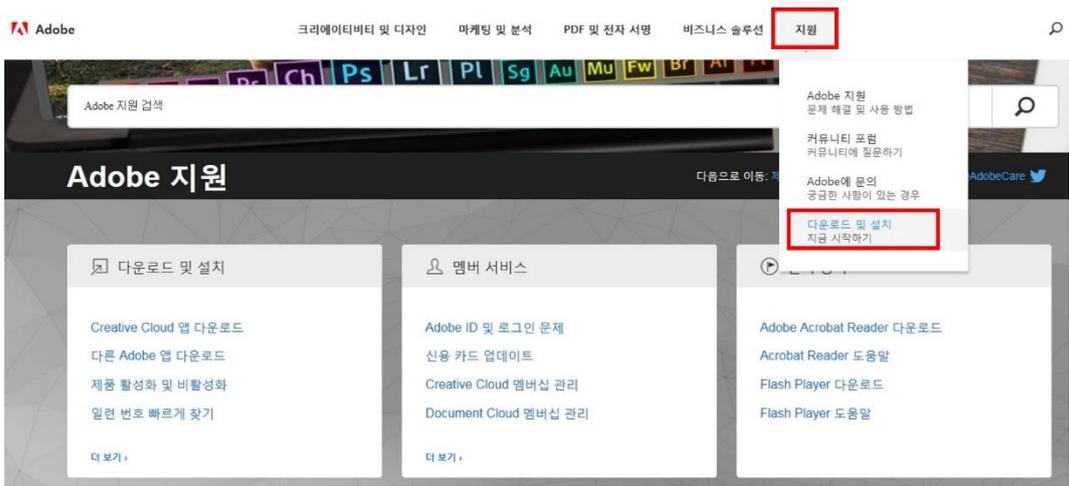
[그림 8] 한컴 자동 업데이트 설정

4. 어도비(Adobe) 제품에 보안 업데이트 적용하기

인터넷을 이용하는 곳이라면 어도비 관련 업데이트 적용도 필수다. 대내외 문서 공유를 위해 PDF 를 이용하는 경우가 대부분이고, 어도비 플래시 취약점은 공격자들이 자주 이용하는 단골 메뉴이기 때문이다. 어도비 보안 패치 또한 어도비 홈페이지에서 확인 및 이용할 수 있다.

(<https://www.adobe.com/kr/downloads/updates.html>)

▶ 어도비 홈페이지 > [지원] > [다운로드 및 설치] > [제품 업데이트] > 사용 중인 제품 선택 후 최신 버전 업데이트 다운로드



[그림 9] 어도비 홈페이지 '다운로드 및 설치' 메뉴

직원들이 패치를 적용했는지 확인하려면?

누구나 쉽게 따라할 수 있는 가이드를 배포하더라도 보안 관리자에게는 한 가지 과제가 남는다. 실제로 패치 업데이트를 한 직원들이 얼마나 있는지, 여전히 적용하지 않은 직원들은 누구인지를 파악하는 것이다. 그렇다고 한창 일하고 있는 직원들의 자리로 찾아가 일일이 PC를 확인할 수도 없는 노릇. 이럴 때 그 자리에서 쉽고 간편하게 전사 패치 적용 현황을 한눈에 확인하고 필요 시 알림 메시지를 보낼 수 있는 '안랩 내 PC 지키미'를 활용하자.

안랩 내 PC 지키미는 수십~수백 대 이상의 업무용 PC의 보안 상태를 중앙에서 점검하고 필요 시 자동 또는 관리자가 강제 조치까지 할 수 있는 'PC 취약점 점검 및 자동 조치 솔루션'이다. 안랩 내 PC 지키미는 취약점 이용 공격 예방은 물론, 주요 컴플라이언스 준수와 관련된 72개 보안 점검 항목 및 조치를 제공한다. 패치뿐만 아니라 ▲화면 보호기 설정 여부 ▲비밀번호 설정 여부 ▲액티브 X 설치 여부 ▲CMOS 패스워드 설정 여부 등도 점검할 수 있으며, 기업 및 기관의 필요에 따라 관리자가 점검 항목을 추가할 수 있다.

1. 안랩 내PC지키미로 패치 적용 여부 확인하기

[그림 10]은 업무용 PC 사용자가 볼 수 있는 안랩 내 PC 지키미 화면으로, 백신 설치 및 최신 엔진 사용 여부를 비롯해 운영체제, MS 오피스, 한글 프로그램 등의 최신 보안 패치 적용 여부를 손쉽게 확인할 수 있다.

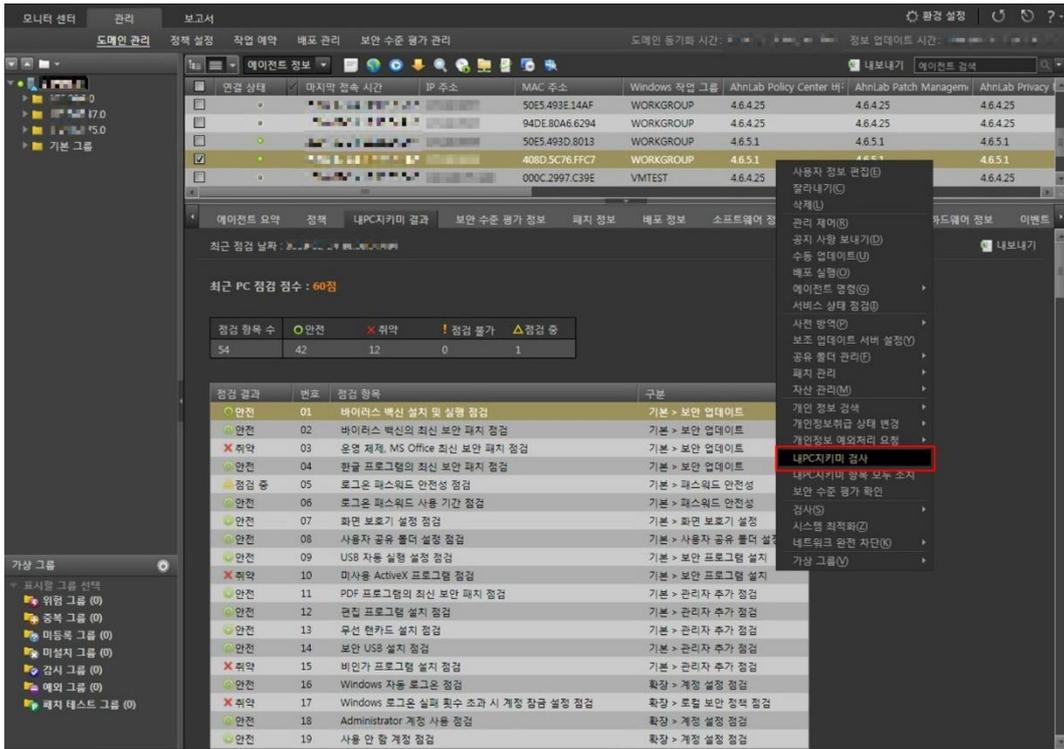
안랩 내 PC 지키미가 각광받는 가장 큰 이유는 보안 관리자는 물론 PC 사용자도 거의 아무것도 하지 않아도 된다는 점이다. 최신 보안 패치가 적용되어 있는지 확인하기 위해 안랩 내 PC 지키미를 실행하지 않아도 지정된 날짜나 일정한 기간마다 자동으로 PC의 패치 적용 여부를 검사한다.



[그림 10] 안랩 내 PC 지키미 사용자 화면

점검 결과 최신 패치가 적용되어 있지 않으면 [그림 10]의 오른쪽 화면과 같이 해당 항목이 “취약”으로 표시되고 사용자의 조치를 유도한다. 이때 사용자가 해당 항목을 클릭하면 화면 하단에 구체적인 조치 방법에 대한 안내와 함께 해결하기 버튼이 나타난다. 이 버튼을 한번만 클릭하는 것으로 소프트웨어 제조사 페이지 등으로 즉시 연결되어 손쉽게 패치를 다운로드 할 수 있다.

보안 관리자가 전사 또는 특정 PC에 대해 패치 적용 여부를 점검할 수도 있다. 관리자는 [그림 11]과 같은 관리자 화면에서 패치 검사 또는 그 외 원하는 점검 항목을 선택한 후 ‘내 PC 지키미 검사’를 클릭하면 된다. 검사 결과 패치 적용이 취약한 상태로 확인된 PC에 대해서는 알림 메시지를 발송하여 사용자의 조치를 유도할 수 있다.



[그림 11] 안랩 내 PC 지키미 관리자 화면

2. '원클릭'으로 즉각 보안 패치 적용하기: PMS 연동

해결하기 버튼을 통해 이동하여 패치를 다운로드하는 것도 번거롭다고 느낄 수 있다. 만일 패치 관리 솔루션인 '안랩 패치 매니지먼트(AhnLab Patch Management, APM)'를 사용 중인 기업 및 기관이라면 더욱 간단한 패치 적용이 가능하다.

안랩 패치 매니지먼트가 연동되어 있는 경우, "취약"으로 표시된 항목에 대해 사용자가 해결하기 버튼을 클릭하면 적용해야 할 패치 리스트를 즉시 확인 및 다운로드 할 수 있다. 마찬가지로 중앙에서 보안 관리자가 패치 여부를 점검 후 취약한 PC 에 대해 강제로 패치 적용을 실행할 수 있다. 백신(V3)과 윈도우 운영체제뿐만 아니라 MS 오피스 제품군, 인터넷 익스플로러(Internet Explorer), 한글, 어도비(Adobe), 자바(Java) 등의 최신 패치를 자동 또는 수동으로 적용해 사내 PC 를 항상 '안전' 상태로 유지할 수 있다.

안랩 내 PC 지키미와 안랩 패치 매니지먼트를 연동했을 때의 가장 큰 장점은 패치를 '자동'으로 적용할 수 있다는 점이다. 일부 패치 관리 제품(PMS)은 보안 관리자가 소프트웨어 제공사의 웹사이트나 PMS 업체를 통해 패치를 다운로드 또는 전달 받아 사내 서버나 관리자 페이지 또는 공유 폴더에 올려야 사내 배포가 가능하다.

반면 안랩은 자사 서버를 통해 패치 파일을 자동으로 고객사의 서버로 전달하고 고객사 정책에 따라 각 시스템에 패치를 자동으로 다운로드한다. 말 그대로 '자동 패치'를 제공하기 때문에 별도의 조작이 필요하지 않아 관리자뿐만 아니라 사용자도 거의 부담이나 불편함을 느끼지 않는다. 또한 국정원 권고 패치 관리와 불법 소프트웨어 사용 현황까지 점검 및 조치가 가능하다는 것도 매력이다.

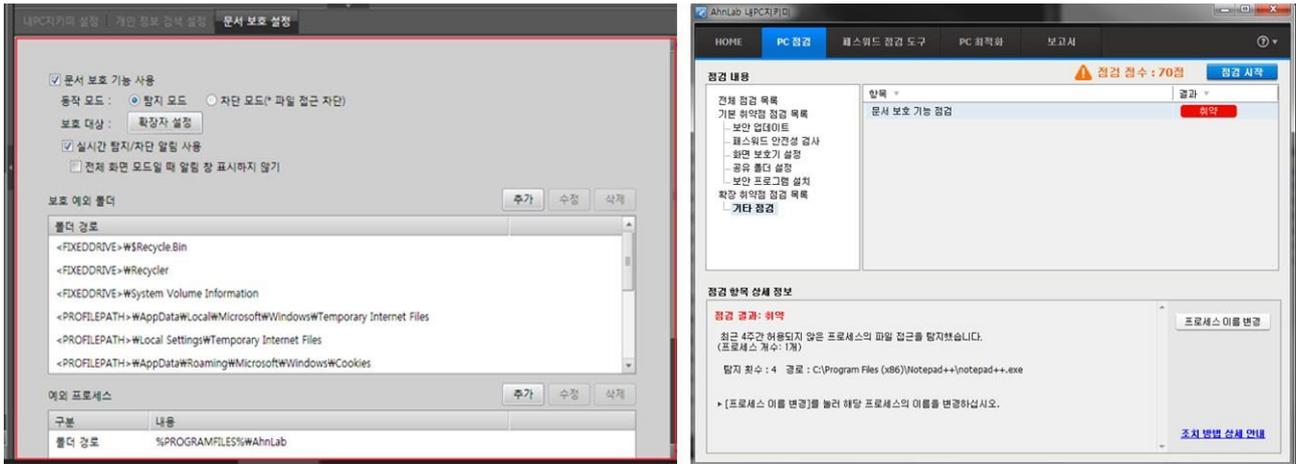
▶ ['안랩 패치 매니지먼트' 더 알아보기](#)

3. 랜섬웨어 피해 예방을 위한 추가 기능: 문서 보호

예전부터 취약점을 이용한 공격이 지속적으로 발생해왔음에도 불구하고 최근 들어 더욱 패치 적용이 강조되는 이유는 랜섬웨어 때문이다. 안랩 내 PC 지키미는 최신 패치 적용 여부 검사 및 조치가 가능하다는 점 외에도 랜섬웨어 피해 예방에 상당한 도움을 주는 기능도 제공하고 있다. 바로 "문서 보호" 기능이다.

문서 보호 기능이란 '.doc', '.docx', '.xls' 등의 확장자를 가진 주요 문서 파일에 대해 생성, 쓰기, 덮어쓰기, 파일명 변경, 삭제 등을 시도하는 프로세스를 탐지하고, 이를 허용 또는 차단함으로써 중요 문서의 훼손 또는 변조를 방지하는 기능이다. 랜섬웨어가 파일을 암호화하는 프로세스도 일부 차단할 수 있어 랜섬웨어 피해 예방 효과를 기대할 수 있다.

[그림 12]는 안랩 내 PC 지키미의 문서 보호 설정 화면으로, 왼쪽의 관리자 화면에서 '문서 보호 기능 사용'을 설정하면 오른쪽과 같이 사용자 화면의 '기타 점검 항목'에서 문서 보호 기능 사용 여부를 확인할 수 있다.



[그림 12] 관리자 화면(왼쪽) 및 사용자 화면(오른쪽)의 문서 보호 기능 설정

문서 보호 기능이 적용된 PC 의 문서에 의심스러운 프로세스가 접근할 경우 알림창이 나타난다. 또한 사용자 화면의 취약 항목 점검 결과를 통해 의심스러운 프로세스 접근 내역에 대한 상세 정보도 제공한다.

패치 관리부터 임직원 보안 인식 개선까지

랜섬웨어를 비롯한 각종 악성코드 감염 피해를 예방하는 첫 걸음은 '패치 관리'다. 그러나 아무리 엄격한 보안 정책을 적용하고 수시로 PC 보안 관리의 중요성을 강조한들 업무로 바쁜 임직원들에게 패치 적용은 번거롭고 우선순위가 낮은 일로 치부되기 십상이다. 반면 사내에서 사용 중인 수많은 프로그램의 종류와 버전도 다양하기 때문에 보안 관리자로서는 이를 파악하는 것부터도 쉽지 않다.

안랩 내 PC 지키미와 안랩 패치 매니저먼트의 연동을 통해 보안 관리자는 물론 보안이나 컴퓨터 관련 이해가 적은 사용자들도 부담 없이 손쉽게 패치 적용 여부를 확인하고 조치할 수 있어 기업의 랜섬웨어 피해 예방 및 궁극적인 보안 수준을 한 단계 업그레이드 할 수 있다. 쉽고 간편한 조치와 더불어 PC의 보안 상태를 점수와 직관적인 UI로 보여준다는 점 때문에 임직원들의 보안 인식 개선 효과까지 기대할 수 있다.

AhnLab

AhnLab Inc.

경기도 성남시 분당구 판교역로 220 (우) 13493 | 대표전화 : 031-722-8000

www.ahnlab.com

© AhnLab, Inc. All rights reserved.